

United States District Court
for the
Western District of New York

In the Matter of the Search of

(Briefly describe the property to be searched or identify the person by name and address.)

The Premises Known as **104 York Street, Apartment 1, Buffalo, New York**
and

Case No. 20-MJ- 144

The Safe Deposit Box Associated with Account **3337001955**,
located at Bank of America, 4049 Seneca Street, West Seneca, New York 14224

APPLICATION FOR SEARCH WARRANTS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*: See Attachment A-1, which is attached hereto and incorporated by reference herein, located in the Western District of New York, there is now concealed *(identify the person or describe the property to be seized)*: Evidence, fruits, and instrumentalities pertaining to violations of Title 18, United States Code, Sections 1343, 1344, and 1349, as more fully set forth in Attachment B-1, which is attached hereto and incorporated by reference herein.

I, a federal law enforcement officer or an attorney for the government, request a second search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*: See Attachment A-2, which is attached hereto and incorporated by reference herein, located in the Western District of New York, there is now concealed *(identify the person or describe the property to be seized)*: Evidence, fruits, and instrumentalities pertaining to violations of Title 18, United States Code, Sections 1343, 1344, and 1349, as more fully set forth in Attachment B-2, which is attached hereto and incorporated by reference herein.

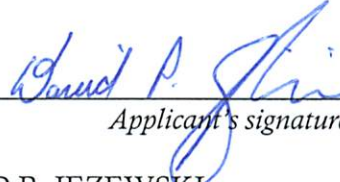
The basis for each search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

Each search is related to violations of Title 18, United States Code, §§ 1343, 1344, and 1349 *[statutory violation(s)]*.

The application is based on these facts:

- ☒ continued on the attached sheet.
- ☐ Delayed notice of ____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature

DAVID P. JEZEWSKI
SPECIAL AGENT
HOMELAND SECURITY INVESTIGATIONS

Printed name and title

Sworn to before me and signed telephonically.

Date: September 16, 2020



Judge's signature

City and state: Buffalo, New York

HONORABLE H. KENNETH SCHROEDER, JR.
UNITED STATES MAGISTRATE JUDGE

Printed name and Title

AFFIDAVIT

STATE OF NEW YORK)
COUNTY OF ERIE) SS:
CITY OF BUFFALO)

I, David P. Jezewski, being duly sworn, deposes and states as follows:

1. I am a Special Agent with Homeland Security Investigations (HSI) within the Department of Homeland Security, assigned to the office of the Special Agent in Charge, Buffalo, New York, and have been so employed since 2005. Prior to that, I was employed by United States Customs and Border Protection as an Officer in Nogales, Arizona.

2. As part of my duties as a Special Agent with HSI, I investigate financial crimes involving fraud schemes pertaining to wire fraud in violation of Title 18, United States Code, Section 1343; bank fraud in violation of Title 18, United States Code, Section 1344; and conspiracies to commit wire fraud and bank fraud in violation of Title 18, United States Code, Section 1349.

3. This affidavit is submitted in support of an application to search the residence known as 104 York Street, Apartment 1, Buffalo, New York 14213 (hereinafter referred to as the SUBJECT PREMISES) and a safe deposit box associated with Bank of America safe deposit box account 3337001955, located at 4049 Seneca Street, West Seneca, New York 14224 (hereinafter referred to as SUBJECT SAFE DEPOSIT BOX) for evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Section 1343 (wire fraud); Title

18, United States Code, Section 1344 (bank fraud); and Title 18, United States Code, Section 1349 (conspiracy to commit wire fraud and bank fraud) (hereinafter, “the Subject Offenses”), all as more fully described in Attachments B-1 and B-2. The SUBJECT PREMISES, as further described and depicted in Attachment A-1, is a two (2) story residence with tan siding and brown trim. The SUBJECT SAFE DEPOSIT BOX, as further described in Attachment A-2, is a safe deposit box located at Bank of America, 4049 Seneca Street, West Seneca, New York 14224.

4. The statements contained in this affidavit are based upon my investigation, information provided to me by other law enforcement personnel, including but not limited to Special Agents of HSI located in Buffalo, New York, and on my experience and training as a special agent of HSI. Because this affidavit is being submitted for the limited purpose of establishing probable cause to secure two search warrants, I have not included each and every fact known to me concerning this investigation. Rather, I have set forth facts that I believe are necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of violations of the Subject Offenses are presently located at the SUBJECT PREMISES and in the SUBJECT SAFE DEPOSIT BOX. Based on the facts set forth in this affidavit, I respectfully submit there is probable cause to believe that there is presently concealed, within the SUBJECT PREMISES and the SUBJECT SAFE DEPOSIT BOX, the items described in Attachments B-1 and B-2, which constitute evidence, fruits, and instrumentalities of violations of the Subject Offenses.

PROBABLE CAUSE

7. The investigation described in this affidavit concerns a “Business Email Compromise” (BEC) scam. Your affiant has learned through training and experience that BEC fraud is a type of scam typically targeting companies that conduct wire transfers and have suppliers and vendors abroad. Based on my training and experience, I know that BEC scams are typically carried out in the following manner: Scammers use techniques, such as keyloggers and phishing attacks, to compromise or spoof the corporate or publicly available email accounts of executives or high-level employees who are involved in a company’s finances or wire transfer payments to vendors. BEC attackers often rely heavily on social engineering tactics to trick unsuspecting employees and executives. Often, they impersonate the CEO or any executive authorized to do wire transfers. In addition, BEC scammers also typically carefully research and closely monitor their potential target victims and their organizations. Once the scammer has obtained access to a victim’s email account, the scammer can then alter the victim company’s payment invoices so that vendor payments will be directed to a bank account controlled by the scammer, rather than a bank account controlled by the legitimate, intended payee. As described below, there is probable cause to believe that evidence within the SUBJECT PREMISES and SUBJECT SAFE DEPOSIT BOX has been used in connection with, and in furtherance of, a BEC fraud committed on a number of victims.

BACKGROUND OF INVESTIGATION

A. Ahmed MUSA's Involvement in BEC Activity

8. On or about February 26, 2020, HSI Buffalo received information from Citizens Bank stating that a business account opened on June 17, 2019 in Buffalo, New York was the subject of a suspected BEC fraud utilizing checking account **4020430933** at Citizens Bank. Citizens Bank account number **4020430933** was registered to Jasa Cipta Rembaka LLC, 1420 Hertel Avenue, Buffalo, New York, 14216 and alleged to be operating as an insurance carrier specializing in accident and health insurance. Citizens Bank provided information that on or about June 26, 2019, Victim 1, Willis Towers Watson (hereinafter referred to as "WTW"), sent a wire transfer in the amount of \$131,636.39 to Jasa Cipta Rembaka LLC, Citizens Bank account number **4020430933**. Citizens Bank provided information that on or about December 6, 2019, Victim 2, Rutherford Wine Co. (hereinafter referred to as "RWC"), sent a wire transfer in the amount of \$112,912.02 to Jasa Cipta Rembaka LLC, Citizens Bank account number **4020430933**.

9. Citizens Bank provided your affiant with a copy of the business checking application used to open Citizens Bank business checking account **4020430933**. The documents contain, in part, the following information:

- Corporation filing receipts from the New York State Division of Corporations and State Records, registering Jasa Cipta Rembaka LLC, 1420 Hertel Avenue, Buffalo, New York 14216, as a limited liability company, filed by Ahmed MUSA on June 17, 2019.

- Citizens Bank business checking application for account **4020430933** listed Jasa Cipta Rembaka LLC, 1420 Hertel Avenue, Buffalo, New York 14216, signed by Ahmed MUSA on June 17, 2019, and listing him as the sole member on the account.

10. Citizens Bank provided your affiant with statements for Citizens Bank account **4020430933** from June 17, 2019 to December 9, 2019. The following graph shows wire transfers and check withdrawals that occurred in account **4020430933** during this period.

Date	Transaction	Debits	Credits
6/17/2019	Account opening deposit		\$60.00
6/26/2019	Incoming wire transfer		\$131,636.39
6/26/2019	Check withdrawal	\$80,000.00	
7/2/2019	Check withdrawal	\$45,000.00	
7/5/2019	Cash withdrawal	\$5,000.00	
8/13/2019	Cash deposit		\$20,765.00
8/14/2019	Outgoing wire transfer	\$20,765.00	
9/4/2019	Cash deposit		\$20,060.00
9/4/2019	Outgoing wire transfer	\$20,000.00	
12/6/2019	Incoming wire transfer		\$112,912.02
12/6/2019	Check withdrawal	\$65,000.00	
12/9/2019	Account close out check	\$47,832.00	

11. Citizens Bank provided your affiant with check copies that were issued on June 26, 2019 (\$80,000.00), July 2, 2019 (\$45,000.00), December 6, 2019 (\$65,000.00) and December 9, 2019 (\$47,832.00). All four (4) checks were cashed at Castleway Financial, 380 Connecticut Street, Buffalo, New York 14213 and signed by Ahmed MUSA on the same day they were issued by Citizens Bank. MUSA also wrote social security number 081-94-8582 and telephone number 716-870-6438 on the back of the checks cashed on June 26, 2019 for \$80,000.00 and December 9, 2019 for \$47,832.00. Castleway Financial is a money service

business that offers multiple services including check cashing, money transfers, money orders and prepaid cards.

12. Your affiant has learned through his training and experience that legitimate businesses utilize a bank in the normal course of business to avoid high fees and to monitor costs that affect company profit. For a legitimate business to utilize a check cashing business, like Castleway Financial, which often charge high fees, would not make good business sense. This supports the conclusion that Jasa Cipta Rembaka LLC is a shell company formed in order to facilitate criminal conduct.

13. Citizens Bank provided documentation for the outgoing wire transfers that occurred on August 14, 2019 and September 4, 2019. The outgoing wire for \$20,765.00 on August 14, 2019 was sent to Wellfull Group Co LTD in Hangzhou, China for the purchase of cars. The outgoing wire for \$20,000.00 on September 4, 2019 was sent to Tianjin Tiankai Chemical Industries in Tianjin, China for industrial materials. Your affiant believes these outgoing wire transfers are not consistent with a business that alleges to be operating as an insurance carrier specializing in accident and health insurance.

14. Your affiant conducted a physical address check at 1420 Hertel Avenue, Buffalo, NY 14216 and identified a soccer bar and restaurant in Buffalo, New York. An internet search of this address identified the same.

15. Your affiant conducted a search of the Citizen Law Enforcement Analysis and Reporting (CLEAR) database and identified Ahmed MUSA, DOB: 11/9/1990, SSN 081-94-8582, phone number 716-870-6438 and an address of 104 York Street, Apt 1, Buffalo, New York 14213.

16. Your affiant conducted an internet search of victim 1, WTW, and identified a company that provides insurance agent and broker services for a range of insurance types. On August 31, 2020, your affiant attempted to email WTW in Singapore to confirm that they were a victim of the fraudulent activity resulting in a loss of \$131,636.39. Your affiant was contacted by an attorney of WTW Global Investigations in Nashville, TN who stated that he was referred your affiant's inquiry through WTW in Singapore. The attorney for WTW in Nashville, TN stated he would investigate the details of the wire for \$131,636.39 and provide an update to your affiant. On September 10, 2020 your affiant spoke with the attorney from WTW in Nashville, TN who confirmed that the wire for \$131,636.39 was re-directed to Citizens Bank account number **4020430933** based on a fraudulent email received by a representative at WTW in Singapore. Specifically, the attorney for WTW stated that:

Willis Singapore has a client by the name of Jasa Cipta Rembaka LLC ("JCR"). As of June 13, 2019, Willis Singapore understood that JCR's bank account was an account at [a bank other than Citizens Bank]. On June 14, 2019, [K.W.], a Willis employee, received an email from a person purporting to be B. Eko Martinko from an email account with a slight variation saying that the JCR bank account had been changed to an account at [Citizens Bank]. On June 26, 2019, Willis Singapore wired \$131,636.39 to the account at [Citizens Bank]. On or about December 17, 2019, [K.W.] was contacted by the actual person B. Eko Martinko and advised that no change in the bank account had been authorized.¹

¹ The attorney for WTW originally stated that the bank to which the BEC scammer directed funds was JPMorgan Chase Bank and that WTW's true, correct account was held at Citizens Bank. Upon

17. Your affiant conducted an internet search of Jasa Cipta Rembaka and identified a company in Jakarta, Indonesia that offers a wide spectrum of reinsurance services, including expertise in designing and negotiating Treaty Reinsurance. Your affiant was unable to identify a location for Jasa Cipta Rembaka in Buffalo, New York.

18. Your affiant conducted an internet search of victim 2, RWC, and identified a winery in St. Helena, California. On June 23, 2020, your affiant attempted to call RWC to confirm that they were a victim of fraudulent activity resulting in a loss of \$112,912.02 that occurred on December 6, 2019. Your affiant spoke with an accountant at RWC who explained that RWC was a victim of the wire fraud for \$112,912.02 that occurred on December 6, 2019. Citizens Bank also provided your affiant a copy of a recall message from RWC's bank to Citizens Bank dated December 6, 2019. The recall message stated, "Urgent: Fraudulent Payment / Email Spoofing. Please return funds."

B. Eric IWU's Involvement in BEC Activity

19. On or about October 28, 2018, HSI Buffalo received information from Wells Fargo Bank stating that a victim in Dubai, UAE was the subject of a Business Email Compromise (BEC) fraud utilizing checking account number **5566884424** at Wells Fargo Bank. Wells Fargo Bank provided information that on or about August 27, 2018, the victim, SEPCO Electric Power Construction Corporation (hereinafter referred to as "SEPCO"), sent

further inquiry, the attorney for WTW observed that the BEC scammer directed funds to an account at Citizens Bank (rather than JPMorgan Chase), which was different than the bank at which WTW held its true, correct account.

a wire transfer in the amount of \$461,612.00 to Zeeco Inc, Wells Fargo Bank account number **5566884424**. The victim, SEPCO, utilized Emirates NBD Bank to send the wire transfer to Wells Fargo Bank account number **5566884424**. Wells Fargo Bank provided your affiant with documentation showing the wire transfer details from Emirates NBD Bank to Zeeco Inc, account number **5566884424**. On or about September 20, 2018, Wells Fargo received a recall from Emirates NBD Bank requesting that the wire transfer be returned at the request of SEPCO. SEPCO claimed the wire transfer was not intended for the beneficiary account and that the fraudulent credit party details were provided to SEPCO under a hacked email. Wells Fargo Bank provided your affiant with documentation showing the recall from Emirates NBD Bank. The wire recall from Emirates NBD Bank was denied from Wells Fargo Bank because all the funds were depleted from Wells Fargo Bank account **5566884424**. Wells Fargo Bank provided additional information that Wells Fargo Bank account **5566884424** was in the name of Laura STARR, of Los Gatos, California.

20. An internet search of Zeeco Inc identified a company with an exact name match in Broken Arrow, Oklahoma. The website for Zeeco Inc represented the company as a global provider of combustion equipment and advanced environmental systems. On October 31, 2018, your affiant contacted via phone and spoke with the CFO from Zeeco Inc in Broken Arrow, Oklahoma. The CFO of Zeeco Inc stated that the victim, SEPCO, is a customer and that he/she is aware of the wire transfer on August 28, 2018, that SEPCO, claimed to be fraudulent. The CFO of Zeeco Inc provided your affiant emails and documents from SEPCO, confirming SEPCO sent a wire transfer for \$461,612.00 based on a fraudulent email SEPCO received on August 4, 2018, requesting payment. The CFO of Zeeco Inc stated

that SEPCO did not inquire about the fraudulent email or wire instructions on the invoice, before sending the wire on or about August 27, 2018.

21. Wells Fargo provided your affiant with details of outgoing wire transfers from Wells Fargo Bank account **5566884424**. HSI has identified two (2) domestic wire transfers that were sent from Wells Fargo Bank account **5566884424** to the same beneficiary in the United States within days of receiving the incoming wire transfer for \$461,612.00.

Wire 1 – Curtume J Kempe LLC

22. On or about August 30, 2018, Laura STARR sent a \$100,000.00 wire transfer from Wells Fargo Bank account **5566884424** to Northwest Bank account **3706055369**, in the name of Curtume J Kempe LLC. Northwest Bank provided your affiant documentation showing the wire transfer for \$100,000.00 from Wells Fargo Bank account **5566884424** to Northwest Bank account **3706055369**.

23. Northwest Bank provided your affiant with a copy of the business checking application used to open Northwest Bank business checking account number **3706055369**. The Northwest Bank business checking account application listed Curtume J Kempe LLC, 686 Eggert Road, Buffalo, New York 14215, signed by Meshach IHEANACHO on May 7, 2018, and listing him as the sole member on the account. Northwest Bank provided information that Northwest Bank checking account **3706055369** was opened on May 7, 2018 at Northwest Bank located at 690 Kenmore Avenue, Buffalo, New York 14216.

24. Northwest Bank provided your affiant video surveillance from August 31, 2018, inside Northwest Bank located at 690 Kenmore Ave., Buffalo, New York 14216. In the video your affiant identified Meshach IHEANACHO and Eric IWU entering the bank, sitting next to each other in the waiting area and meeting with a Northwest Bank representative in her office together.

25. On November 8, 2018, the Honorable H. Kenneth Schroeder, United States Magistrate Judge for the Western District of New York, issued seizure warrant 18-MC-41 for Northwest Bank Account Number **3706055369** in the name of Curtume J Kempe LLC, upon a finding of probable cause that the bank account was subject to seizure and forfeiture pursuant to Title 18, United States Code, Sections 981(a)(1)(C) and (b) and Title 21, United States Code, Section 853(f) for a violation of Title 18, United States Code, Sections 1343 (wire fraud) and 1344 (bank fraud). On November 28, 2018, your affiant received an official check from Northwest Bank for \$90,587.14 pursuant to the seizure warrant issued by the Honorable H. Kenneth Schroeder on November 8, 2018.

Wire 2 – Crystal Networks Holdings LLC

26. On or about August 30, 2018, Laura STARR sent a \$200,000.00 wire transfer from Wells Fargo Bank account **5566884424** to Bank of America account **226005530692**, in the name of Crystal Networks Holdings LLC. Wells Fargo Bank provided your affiant documentation showing the wire transfer for \$200,000.00 from Wells Fargo Bank account **5566884424** to Bank of America account **226005530692**.

27. Bank of America provided information to your affiant that Bank of America account **226005530692** was opened on April 27, 2018 in Washington, D.C. under the name Crystal Networks Holding LLC and listed 686 Eggert Road, Buffalo, New York 14215 as the mailing address on the account. Bank of America included information that Bank of America account **226005530692** received a wire for \$200,000.00 from Wells Fargo Bank account **5566884424** on August 28, 2018. Bank of America provided your affiant a spreadsheet of all wire activity in Bank of America account **226005530692** since account opening on April 27, 2018. The spreadsheet is shown below for reference:

Date	Debit Wire	Credit Wire	Beneficiary	Beneficiary Bank	Beneficiary Account
9/7/2018	\$154,510.00		H V PLAS CO LTD	Kasikorn Bank Public Co LTD	4642656908
9/7/2018	\$35,000.00		KRISPY KREME DOUGHNUT COMPANY LLC	Citizens Bank	4018732235
8/28/2018		\$200,000.00	CRYSTAL NETWORKS HOLDING LLC	Bank of America	226005530692
8/15/2018	\$4,950.00		KRISPY KREME DOUGHNUT COMPANY LLC	Citizens Bank	4018732235
6/26/2018	\$16,400.00		PWB GROUP INDUSTRY COMMERCE CO	Bank of China	397458343847
6/21/2018	\$10,604.00		OSSY BLESSING	JP Morgan Chase Bank	213878991
6/21/2018	\$1,100.00		ERIC IWU	Citizens Bank	4019203953

28. On or about October 18, 2018, Citizens Bank provided your affiant information that Citizens Bank checking account **4018732235** was opened on June 22, 2018 at Citizens Bank, 355 Orchard Park Road, West Seneca, New York 14224, under the name Krispy Kreme Doughnut Company LLC. Citizens Bank provided information that the registered owner of Citizens Bank account **4018732235** is Eric IWU, 770 Mill Road, Buffalo, New York 14224. Citizens Bank verified with your affiant that Citizens Bank account **4018732235** did receive a wire for \$35,000.00 on September 7, 2018 and \$4,950.00 on June 15, 2018 from Crystal Networks Holding LLC, Bank of America account **226005530692**. Citizens Bank confirmed with your affiant that as of October 18, 2018, Citizens Bank account **4018732235** had approximately \$8,900.00 remaining in the account that had been placed on hold pending further verification by Citizens Bank.

29. Your affiant conducted a public search of the New York State Division of Corporations and identified Krispy Kreme Doughnut Company LLC with an initial filing date of June 21, 2018 and listed address of 770 Mill Road, Apartment 2C, Buffalo, New York 14224.

30. Your affiant conducted a search of the Citizen Law Enforcement Analysis and Reporting (CLEAR) database and identified Eric IWU, DOB: 8/2/1989, SSN 299-37-6380 with a listed address of 770 Mill Road, Apartment 2C, Buffalo, New York 14224 and 264 George Urban Boulevard, Cheektowaga, New York 14224.

31. On December 4, 2018 your affiant and another HSI Special Agent interviewed

Eric IWU at his residence located 264 George Urban Boulevard, Cheektowaga, New York 14225. Your affiant explained to IWU that he had traced a \$35,000.00 wire transfer to Citizens Bank account **4018732235** for Krispy Kreme Doughnut Company LLC from Bank of America account **226005530692** under Crystal Networks Holding LLC. Your affiant further explained to IWU that the \$35,000.00 wire transfer to his account were proceeds of a fraudulent wire received as part of a BEC in which a victim was identified. IWU told your affiant that he was unaware that the \$35,000.00 wire he received were proceeds of fraudulent activity. Your affiant asked IWU if he was willing to abandon the proceeds he had received from the \$35,000.00 wire transfer so that your affiant could return the funds to the victim. IWU agreed to return any remaining funds in Citizens Bank account **4018732235** to your affiant. Your affiant and another HSI Special Agent met IWU at Citizens Bank located at 700 Thruway Plaza Drive, Cheektowaga, New York 14225. IWU closed Citizens Bank account **4018732235** and abandoned an official check for \$8457.15 made payable to US Customs and Border Protection to your affiant. IWU signed an abandonment form for the \$8457.15 witnessed by your affiant and another HSI Special Agent.

C. Eric IWU's Arrest and Subsequent Communications Between IWU and MUSA

32. On or about January 5, 2020, your affiant learned that Eric IWU was arrested on January 1, 2020 by the Cheektowaga Police Department for aggravated DUI and transferred to the Erie County Holding Center in Buffalo, New York. On April 23, 2020, your affiant requested jail calls and inmate information for Eric IWU, from the Erie County Sheriff's Department. On April 27, 2020, the Erie County Sheriff's Office provided your

affiant jail calls and booking data for inmate Eric IWU.

33. The Erie County Sheriff's Department provided a booking sheet with photo identifying Eric IWU, DOB: 8/2/1989, SSN: 299-37-6380, home address at 264 George Urban Boulevard, Cheektowaga, New York 14224. The individual shown on the booking photo is the same person whom I interviewed on December 4, 2018, and he is also the same person who is seen in the surveillance footage described in paragraph 24.

34. Your affiant reviewed jail calls for Eric IWU and identified multiple calls to phone number 716-870-6438. Your affiant conducted a check of the Citizen and Law Enforcement and Reporting (CLEAR) database for 716-870-6438 and identified Ahmed MUSA, 104 York Street, Apt. 1, Buffalo, New York 14217. Your affiant confirmed that Eric IWU referred to the person in these calls as "Ahmed". Your affiant has learned from the calls that MUSA is in possession of a laptop owned by IWU and frequently checks emails on IWU's behalf.

35. Your affiant listened to a call from January 20, 2020 in which IWU wanted MUSA to call his wife so that she could bring IWU's laptop to MUSA so that he could conduct his business for him. The following is a summary, in part, of that conversation:

IWU: *"Try calling this number, because my phone is connected to my laptop, so all the text messages are going to be on the laptop. The other day she wanted to use my laptop to do something, so I didn't give her my password because I don't want her to know what's going on in there, you know what I mean"*
MUSA: *"Okay, so what's her number"*
IWU: *"716-429-3388"*

36. Your affiant listened to a call from January 31, 2020 in which IWU wanted MUSA to check his laptop and read some text messages to him. The following is a summary, in part, of that conversation:

MUSA: *"Your girl dropped off the laptop"*

IWU: *"Yeah, yeah, I asked her to drop of it off yesterday. So, I'll call you around 6, so we can do something on the laptop. I want you to check the text messages that have been coming to my phone. You tell me the names and everything, and the ones I want you to read, I'll tell you"*

MUSA: *"You know when you start saying numbers you can't talk on the phone, you got to be discreet"*

37. Your affiant listened to a call from February 19, 2020 in which IWU wanted MUSA to pay his credit card bill at Bank of America and find out when the payment on his safe deposit box was due. The following is a summary, in part, of that conversation:

IWU: *"Did you get to Bank of America yet"*

MUSA: *"No bro, today I'm staying here until 5...I'll definitely do it for you tomorrow"*

IWU: *"Try to ask her...when is my safe deposit box due date"*

38. On May 7, 2019, a grand jury subpoena was served on Bank of America for any account or safe deposit box information from May 1, 2019 through May 1, 2020 for Eric IWU. Bank of America returned information of an account profile for Eric O IWU, DOB: 8/2/1989, SSN: 299-37-6380, 264 George Urban Blvd, Buffalo, NY 14225, Account # **3337001955**. Bank of America also provided a branch location of 4049 Seneca Street, West Seneca, New York 14224 for the safe deposit box and a safe deposit box access history, showing IWU accessed safe deposit box **337001955**, twenty-four (24) times from May 17, 2019 through December 20, 2019. (As noted, IWU was arrested on January 1, 2020 and has been detained since that date.)

39. On August 20, 2020, your affiant requested jail calls for Eric IWU from the Erie County Sheriff's Department. On August 21, 2020, the Erie County Sheriff's Office provided your affiant jail calls for inmate Eric IWU.

40. Your affiant listened to a call from August 5, 2020 in which MUSA confirmed with IWU that he paid a yearly rental fee at Bank of America for IWU's safe deposit box. The following is a summary, in part, of that conversation:

MUSA: *"You know the most important thing I had to get done...I paid the thing at the bank"*
 IWU: *"The what...the Bank of America?"*
 MUSA: *"I got in there and they told me I couldn't pay...I talked with a guy behind the counter...I told him this was for my older brother... and I just want to pay his fee by August 17... and the guy said sorry, nothing I can do...so I just talked to him, and talked to him and slapped the money in his hand and gave him the account number and asked if he could pay it...and, he did it"*
 IWU: *"How much was it"*
 MUSA: *"It was like 82 dollars...and you know what I did... so when he came back I gave him an extra 50 dollars"*
 IWU: *"So he told you it was meant for the safe deposit box"*
 MUSA: *"Ya, I gave him the number and everything...and he came back outside and gave me the receipt. The most important shit I was scared about, I handled it today."*
 IWU: *"Yo, I was really thinking about that. You did that shit for me, bro, I love you man, thanks bro."*

41. Your affiant listened to a call from August 6, 2020 in which MUSA and IWU were discussing how to move IWU's cars from IWU's house to his attorneys' office. MUSA and IWU also spoke how important it was that IWU's safe deposit box fee was paid. The following is a summary, in part, of that conversation:

IWU: *"When you open the car, try to check the pigeon hole and everything...I put the documents in there...just grab my whole documents and everything...and I think I have some money in there too...all those documents are very important. Also, when you open the trunk...on the sides of the car where you put the stuff to jack the car...try and check in there, I might have some money in there too."*
 MUSA: *"The one thing I was scared of in this whole situation, was your safety deposit box...I made sure I took care of that."*
 IWU: *"Bro, tell me about it, that was really making me not to sleep. So now that's good news"*

right now. Just try to make sure you check the whole car, ...because you know I be putting money in some funny ass way. Try to get the documents and the brown bag.”
MUSA: “I’m going to take the brown bag to my house.”

42. Your affiant listened to a call from August 10, 2020 in which MUSA was explaining to IWU how he moved IWU’s cars from IWU’s house to his attorneys’ office. The following is a summary, in part, of that conversation:

MUSA: “I looked all over the car and couldn’t find nothing. I took all your paperwork and put it in the brown bag and brought it to my house...I checked the trunk where you put the jack and didn’t find anything.”
IWU: “No, I think I have money in the car, I think I put money somewhere in the car, a lot of money, somewhere.
MUSA: “Where do you think you put it?”
IWU: “Did you try under the carpets...and did you try under the seats?”
MUSA: “I could do that tomorrow; I didn’t check under the seats.”

43. Your affiant has not identified more recent calls between MUSA and IWU discussing IWU’s laptop. However, your affiant has also not identified calls between MUSA and IWU suggesting or stating that MUSA no longer possesses IWU’s laptop.

C. Communications Between Eric IWU and Breia IWU

44. Your affiant reviewed jail calls for Eric IWU and identified multiple calls to phone number 716-429-3388. Your affiant conducted a check of the Citizen and Law Enforcement and Reporting (CLEAR) database for 716-429-3388 and identified Breia IWU, 264 George Urban Boulevard, Cheektowaga, New York 14225. Your affiant has learned from the calls that Breia IWU is married to Eric IWU and they have discussed getting a divorce since Eric IWU was arrested on January 1, 2020.

45. Your affiant listened to a call from April 10, 2020 in which Breia IWU told Eric IWU that she moved out and was demanding that she is taking the red car that Eric IWU bought her. The following is a summary, in part, of that conversation:

Eric IWU: *"We already talked about what we are going to do. What I don't want to do is fight with you about anything."*
 Breia IWU: *"Okay, then give me the car"*
 Eric IWU: *"Listen Breia"*
 Breia IWU: *"Give me the car. All I want to hear is that you're giving me the red car or we'll be fighting about it, period"*
 Eric IWU: *"Breia, do you know how much I spent on that car? I spent \$10,000.00 on that car"*
 Breia IWU: *"It doesn't matter. We're married and you bought that car for me. Let me explain something to you. When you go to court, how are you going explain how you got that money...hmmm..."*
 Eric IWU: *"Let's stop talking about all this shit, come on"*

E. Additional activity at Castleway Financial

46. On May 3, 2019, your affiant and another HSI Special Agents interviewed personnel at Castleway Financial located at 380 Connecticut Street, Buffalo, New York, 14213. Your affiant received information that the following cashier's checks were cashed at Castleway Financial located at 380 Connecticut Street, Buffalo, New York 14213. (This summary does not identify all suspicious checks that your affiant believes to have been cashed at Castleway Financial.)

- 3/25/2019 - \$47,000.00 check made payable to CARTIER SAADA SA LLC
- 3/19/2019 - \$67,000.00 check made payable to CARTIER SAADA SA LLC
- 3/13/2019 - \$10,000.00 check made payable to John KAMARA
- 3/11/2019 - \$44,500.00 check made payable to GUNES DINAMIK LLC
- 2/13/2019 - \$28,287.36 check made payable to GUNES DINAMIK LLC

- 12/28/2018 - \$35,000.00 check made payable to Martins ONYEBUCHI

47. The owner of Castleway Financial stated that he recalled the checks referenced above and became suspicious of a group of people utilizing Castleway Financial to cash large checks. The owner showed your affiant copies of paperwork that Castleway Financial requires to cash corporate checks which include: a corporate check cashing application, indemnification agreement, resolution granting authority to cash company checks, personal guaranty, copy of corporation filing, and copy of identification of individual cashing the check.

48. The owner provided your affiant with copies of required documentation signed by Dorothea DANIELS for the CARTIER SAADA SA LLC cashed checks and Martins ONYEBUCHI for the GUNESS DINAMIK LLC cashed checks.

49. The owner provided copies of required documentation for David AGU who was listed as an authorized representative of CARTIER SAADA SA LLC. The owner told your affiant that when AGU presented a cashier's check payable to CARTIER SAADA SA LLC he asked AGU how he heard of Castleway Financial. The owner stated AGU's reply was that he was referred to Castleway Financial from a friend named Eric IWU.

50. Later that day, your affiant was contacted by the owner of Castleway Financial who stated that Martins ONYEBUCHI was at Castleway Financial trying to cash a check made payable to GUNESS DINAMIK LLC for \$210,000.00, drawn off a Citizens Bank

account. The owner stated that he told ONYEBUCHI that he could not cash the check because he did not have the cash on hand and to return on May 6, 2019 when Castleway Financial had more money. The owner stated that ONYEBUCHI called IWU and explained that he was unable to cash the check. The owner stated that IWU told ONYEBUCHI to ask the owner if he could give him whatever cash he had available and that ONYEBUCHI would pick up the rest on May 6, 2019. The owner explained to ONYEBUCHI that he is not allowed to pay partial amounts out for cashed checks. The owner stated that ONYEBUCHI departed Castleway Financial with the cashier's check and stated he would return on May 6, 2019 to cash the check.

51. On May 3, 2019, your affiant contacted Citizens Bank and learned that the \$210,000.00 check that ONYEBUCHI was trying to cash at Castleway Financial earlier that day was associated to checking account **4018718747** at Citizens Bank under the name GROUPE ALDELIA LLC at 214 E Amherst Street, Buffalo, New York 14214. The Citizens Bank account received an international wire for \$227,655.00 on May 3, 2019. Your affiant was provided video surveillance from Citizens Bank identifying ONYEBUCHI requesting the check for \$210,000.00 payable to GUNESS DINAMIK LLC on May 3, 2019

52. On May 6, 2019, your affiant and another HSI Agent interviewed ONYEBUCHI at his residence located at 214 E Amherst Street, Buffalo, New York 14214. Your affiant told ONYEBUCHI that HSI had information that ONYEBUCHI was in possession of a cashier's check for \$210,000.00 payable to GUNESS DINAMIK LLC. Your affiant further explained to ONYEBUCHI that he believed the source of the funds was

obtained through a BEC scam and asked ONYEBUCHI if he was willing to turn over the check to your affiant so that HSI could verify the source of funds. ONYEBUCHI walked outside to his vehicle and provided your affiant with the \$210,000.00 cashier's check payable to GUNESS DINAMIK LLC.

53. On May 8, 2019, your affiant met with personnel at Citizens Bank located at 1893 Elmwood Ave, Buffalo, NY 14207 and returned the \$210,000.00 cashier's check payable to GUNESS DINAMIK LLC. Citizens Bank redeposited the funds into the account held by GROUPE ALDELIA LLC and placed a hold harmless on the account until funds could be verified with sender.

54. On June 5, 2019, the Honorable Leslie G. Foschio, United States Magistrate Judge for the Western District of New York, issued seizure warrant 19-MC-17 for Citizens Bank Account Number **4018718747** in the name of GROUPE ALDELIA LLC, upon a finding of probable cause that the bank account was subject to seizure and forfeiture pursuant to Title 18, United States Code, Sections 981(a)(1)(C) and (b) and Title 21, United States Code, Section 853(f) for a violation of Title 18, United States Code, Sections 1343 (wire fraud) and 1344 (bank fraud). On June 18, 2019, your affiant received an official check from Citizens Bank for \$227,665.00 pursuant to the seizure warrant issued by the Honorable Leslie G. Foschio on June 5, 2019.

F. Surveillance at 104 York Street, Buffalo, New York 14213

55. On September 10, 2020, your affiant conducted surveillance at 104 York Street, Buffalo, New York 14213. At 3:00 pm your affiant observed an unidentified female (UF) walk from the area of 104 York Street, Buffalo, New York 14213 and get into a grey Toyota Corolla, bearing New York license plate JCL-2487. Your affiant followed the UF and at approximately 3:12 pm the UF arrived and parked across the street of 1420 Hertel Avenue, Buffalo, New York 14216. At approximately 3:15 pm your affiant observed Ahmed MUSA get into the passenger side of vehicle occupied by the UF. Your affiant followed the UF and MUSA to 104 York Street, Buffalo, New York 14213. At approximately 3:30 pm your affiant observed the UF and MUSA exit the vehicle and walk toward 104 York Street, Buffalo, New York 14213.

56. Based on the foregoing, I respectfully submit that there is probable cause to believe that a laptop belonging to Eric IWU (“the SUBJECT LAPTOP”) is within the custody and control of Ahmed MUSA and is located at the SUBJECT PREMISES, which is more fully described in Attachment A-1. There is also probable cause to believe that on the SUBEJCT LAPTOP there is located evidence, contraband, fruits, and instrumentalities of violations of the Subject Offenses, as more fully described in Attachment B-1. There is also probable cause to believe that evidence, contraband, fruits, and instrumentalities of violations of the Subject Offenses, as more fully described in Attachment B-1, will be found within the SUBJECT PREMISES.

57. It is unknown whether MUSA owns or possesses any other laptop in addition to the SUBJECT LAPTOP described in this affidavit. Thus, in the event that, upon entering the SUBJECT PREMISES, multiple laptops reasonably appear to be under MUSA's custody or control, this search warrant requests authorization to seize each and every such laptop so that each and every such laptop may be searched for the items described in Attachment B-1.

58. Based on the foregoing, there is also probable cause to believe that in the safe deposit box associated with safe deposit box account 3337001955, located at Bank of America, 4049 Seneca Street, West Seneca, New York 14224, which is more fully described in Attachment A-2, there is evidence, contraband, fruits, and instrumentalities of violations of the Subject Offenses, as more fully described in Attachment B-2. Because safe deposit boxes may typically only be opened using multiple keys, the requested warrant would authorize the executing agents to open the SUBJECT SAFE DEPOSIT BOX in a manner that may physically damage the box, e.g., by drilling the box.

Searching of Computers and Related Media

59. Your affiant has spoken with a certified Computer Forensics Agent from HSI. This Computer Forensics Agent has received specialized training in connection with searching through computers (and related equipment) for files/data, which may contain information related to the items/materials being sought by this search warrant.

60. Based upon my consultations with the Computer Forensics Agent, I know that searching and seizing information from computer systems and other storage media

(computers, PDAs, cell phones, MP3 Players, etc.) often requires agents to seize most or all the computer system or storage media to be searched later by a qualified computer forensic analyst in a laboratory or other controlled environment. This is true for the reasons set out below.

61. Computer storage media is used to save copies of files and communications, while printers are used to make paper copies of same. Applications and associated data stored on the storage media are the means by which the computer can send, print and save such activity. Finally, password protected data and other security devices are often used to restrict access to or hide computer software, documentation or data. Each of these parts of the computer thus are integrated into the entire operation of a computer. To best evaluate the evidence contained within computers, all related computer equipment described above should be available to the Computer Forensics Agent.

62. In addition to the need to have all of the components available when a search of the computer is undertaken, the search of the computer itself is a time-consuming process. However, unlike the search of documentary files, computers store data in files, which cannot easily be reviewed. For instance, a single 100 gigabyte hard drive is the electronic equivalent of approximately 50,000,000 pages of double-spaced text. Furthermore, software and individual files can be password protected; files may be secluded in hidden directories; files can be mislabeled or be labeled with names which are misleading; similarly, files which contain innocent appearing names (_Smith.ltr_) may actually be electronic commands to electronically self-destruct the data; files can also be deleted (but unlike documents which are

destroyed) the data from deleted electronic files often remain on the storage device until overwritten by the computer. For example, the computer's hard drive stores information in a series of sectors each of which contain a limited number of electronic bytes (usually 512); these sectors are generally grouped to form clusters. There are thousands/millions of such clusters on a hard drive. A file's clusters may be scattered throughout the drive (a portion of a memo could be at Cluster 103 while the next portion of the memo could be stored at Cluster 2057). For a non-deleted file, there are "pointers" which guide the computer in piecing the clusters together. For a file that has been deleted, the "pointers" have been removed. Thus, the forensic examination would include the piecing together of the associated clusters that made up the "deleted" file. Being aware of these pitfalls, the investigator/analyst must follow a potentially time-consuming procedure to review the contents of the computer storage device so as to ensure the integrity of the data and/or evidence. Even if a deleted file has been overwritten and no fragment remains, applications, which provide access to the Internet and operating systems, maintain records (or logs) of activity on the Internet for an indefinite period. Such logs are located in files not usually used and/or accessed by computer users. A single computer and related equipment could take many days to properly analyze.

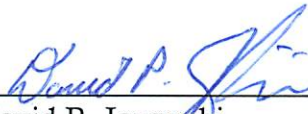
63. Accordingly, there is a reasonable need to remove the computers and computer related equipment to a forensic setting in order to properly conduct a thorough search of the contents. Such action will greatly diminish the intrusion of law enforcement into the premises and will ensure that evidence can be searched for without the risk of losing, destroying or missing the information/data for which there has been authorization to search.

CONCLUSION

64. Based upon the forgoing, the undersigned respectfully submits that there is probable cause to believe that evidence, fruits and instrumentalities of violations of Title 18, United States Code, Section 1343 (fraud by wire, radio or television), Title 18, United States Code, Section 1344 (bank fraud), and Title 18, United States Code, Section 1349 (conspiracy to commit wire fraud and bank fraud) as specifically described in Attachments B-1 and B-2 to this application, are presently located at the SUBJECT PREMISES described in Attachment A-1 and the SUBJECT SAFE DEPOSIT BOX described in Attachment A-2. The undersigned therefore respectfully requests that the attached warrants be issued authorizing a search for the items listed in Attachments B-1 and B-2 at the SUBJECT PREMISES and SUBJECT SAFE DEPOSIT BOX.


REQUEST FOR SEALING

65. I further request that the Court order that all papers in support of this application, including the affidavit and search warrants, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation.



David P. Jezewski
Special Agent
Homeland Security Investigations

Subscribed to and sworn before me, telephonically,
this 16th day of September, 2020.



HON. H. KENNETH SCHROEDER, JR.
United States Magistrate Judge

Attachment A-1

PREMISES TO BE SEARCHED

The subject premises is 104 York Street, Apartment 1, Buffalo, New York. The subject premises is a two (2) story house that has tan siding with brown trim and a brown front door. The number "104" is visible above the front door of the SUBJECT PREMISES. Further, the SUBJECT PREMISES is located at the corner of York Street and Fourteenth Street, Buffalo, New York 14213, on the southwest corner. Apartment 1 is located on the first floor of 104 York Street, Buffalo, New York 14213 with a front and side entrance.



ATTACHMENT A-2

SAFE DEPOSIT BOX TO BE SEARCHED

Bank of America safe deposit box associated to safe deposit box account
3337001955, located at Bank of America, 4049 Seneca Street, West Seneca, New York
14224.

NOTHING MORE AFTER THIS LINE

HKS, 9/16/2020

ATTACHMENT B-1

Items to be Searched for and Seized from the Premises Identified in Attachment A-1

All records, information, and evidence, in whatever form, including the contents of all wire and electronic communications, attachments, stored files, print outs, and header information that are or that contain evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 1343 (wire fraud), 18 U.S.C. § 1344 (bank fraud), and/or 18 U.S.C. § 1349 (conspiracy to commit bank fraud and wire fraud) including:

- a. United States currency;
- b. Schemes to defraud businesses by creating false or fraudulent invoices and/or receipts for payment of services or goods;
- c. All communications, correspondence, or documents related to the creation of bank accounts and/or the location, disbursement, and/or transfer of funds obtained as a result of fraudulent activity;
- d. All communications, correspondence, or documents concerning research about, and investigation of, companies and/or employees of any company;
- e. Efforts or techniques used to obtain access to the email account of any victim company and/or any employee of any victim company;
- f. Genuine or fraudulent invoices and/or receipts for payments of services or goods used to facilitate fraud;
- g. The creation or transfer of false or fraudulent documents;
- h. The creation of limited liability companies (LLCs) or other business entities, such as partnerships and corporations;
- i. All communications between individuals or entities involved in the scheme to defraud;
- j. All communications or attachments related to spoofing technology and techniques intended to conceal fraudulent activity;

- k. Banking and financial institution records, wire transfer records, bank statements, cancelled checks, deposit slips, check registers, records of any money orders, cashier's checks, and official bank checks, savings passbooks and statements of account(s), safe deposit box keys and business and personal ledgers evidencing financial transactions from January 1, 2018 to present.
- l. Records relating to the ownership or renting of off-site storage facilities more particularly described as contracts, receipts, keys, notes, bills and any letters of correspondence from January 1, 2018 to present.
- m. Records evidencing business ownership, occupancy, residency, rental and/or ownership of the premises to be searched, including, but not limited to utility and telephone bills, cable bills, mail envelopes and addressed correspondence.
- n. All computers that are, or that reasonably appear to be, within the custody and control of Ahmed MUSA and Eric IWU. The following items may be seized, and then searched, for all records, information, and evidence identified above, and for all items identified in subparagraph (o):
 - i. Computer hardware, meaning any and all computer equipment owned or used by Ahmed MUSA and Eric IWU. Included within the definition of computer hardware are any electronic devices capable of data processing (such as central processing units, laptop or notebook or netbook or tablet computers, personal digital assistants, gaming consoles, and wireless communication devices to include cellular telephone devices capable of internet access); peripheral input/output devices (such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media); related communications devices (such as modems, wireless routers, cables and connections); storage media, defined below; and security devices, also defined below.
 - ii. Computer software owned or used by Ahmed MUSA and Eric IWU, meaning any and all data, information, instructions, programs, or program codes, stored in the form of electronic, magnetic, optical, or other media, which is capable of being interpreted by a computer or its related components. Computer software may also include data, data fragments, or control characters integral to the operation of computer software, such as operating systems software, applications software, utility programs, compilers, interpreters, communications software, and other programming used or intended to be used to communicate with computer components.
 - iii. Computer related documentation, meaning any written, recorded, printed, or electronically stored material that explains or illustrates the

- configuration or use of any seized computer hardware, software, or related items.
- iv. Data security devices, meaning any devices, programs, or data whether themselves in the nature of hardware or software that can be used or are designed to be used to restrict access to, or to facilitate concealment of, any computer hardware, computer software, computer related documentation, or electronic data records. Such items include user names and passwords; data security hardware (such as encryption devices, chips, and circuit boards); data security software or information (such as test keys and encryption codes); and similar information that is required to access computer programs or data or to otherwise render programs or data into usable form.
 - v. All storage media owned or used by Ahmed MUSA and Eric IWU capable of collecting, storing, maintaining, retrieving, concealing, transmitting, and backing up electronic data. Included within this paragraph is any information stored in the form of electronic, magnetic, optical, or other coding on computer media or on media capable of being read by a computer or computer related equipment, such as fixed hard disks, external hard disks, removable hard disks (including micro drives), floppy diskettes, compact disks (CDs), digital video disks (DVDs), tapes, optical storage devices, laser disks, thumb drives, iPods, digital cameras, memory cards (e.g. CF or SD cards), Xboxes, flash drives, or other memory storage devices. This also includes areas with digital storage capability on devices such as printers, scanners, wireless routers, etc.
 - vi. Routers, modems, and network equipment used to connect computers to the Internet.
- o. For all computer or storage medium whose seizure is authorized by this warrant, and all computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "Computer"):
- i. evidence of who used, owned, or controlled the Computer at the time the things described in this Attachment were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
 - ii. evidence of software that would allow others to control the Computer, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
 - iii. evidence of the lack of such malicious software;

- iv. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;
- v. evidence indicating the computer user's state of mind as it relates to applying for, and spending funds obtained from, PPP loans;
- vi. evidence of the attachment to the Computer of other storage devices or similar containers for electronic evidence;
- vii. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the Computer;
- viii. evidence of the times the Computer was used;
- ix. passwords, encryption keys, and other access devices that may be necessary to access the Computer;
- x. documentation and manuals that may be necessary to access the Computer or to conduct a forensic examination of the Computer;
- xi. records of or information about Internet Protocol addresses used by the Computer;
- xii. records of or information about the Computer Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;
- xiii. contextual information necessary to understand the evidence described in this attachment.

NOTHING MORE AFTER THIS LINE

HKS, 9/16/2020

ATTACHMENT B-2
Items to be Searched for and Seized from the Safe Deposit Box
Identified in Attachment A-2

All records, information, and evidence, in whatever form, that are or that contain evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 1343 (wire fraud), 18 U.S.C. § 1344 (bank fraud), and/or 18 U.S.C. § 1349 (conspiracy to commit bank fraud and wire fraud), including:

- a. United States currency;
- b. Banking and financial institution records, wire transfer records, bank statements, cancelled checks, deposit slips, check registers, records of any money orders, cashier's checks, and official bank checks, savings passbooks and statements of account(s), safe deposit box keys and business and personal ledgers evidencing financial transactions from January 1, 2018 to present;
- c. Schemes to defraud businesses by creating false or fraudulent invoices and/or receipts for payment of services or goods;
- d. All communications, correspondence, or documents related to the creation of bank accounts and/or the location, disbursement, and/or transfer of funds obtained as a result of fraudulent activity;
- e. All communications, correspondence, or documents concerning research about, and investigation of, companies and/or employees of any company;
- f. Genuine or fraudulent invoices and/or receipts for payments of services or goods used to facilitate fraud;
- g. The creation or transfer of false or fraudulent documents;
- h. The creation of limited liability companies (LLCs) or other business entities, such as partnerships and corporations;
- i. All communications between individuals or entities involved in the scheme to defraud; and

This warrant authorizes the executing agents to take all steps necessary to open the safe deposit box (including, but not limited to, drilling the box), which may physically destroy the box and/or render it unable to be reused.

NOTHING MORE AFTER THIS LINE

HKS, 9/16/2020